

Paweł Pokrywka

Kto kontroluje twój modem?

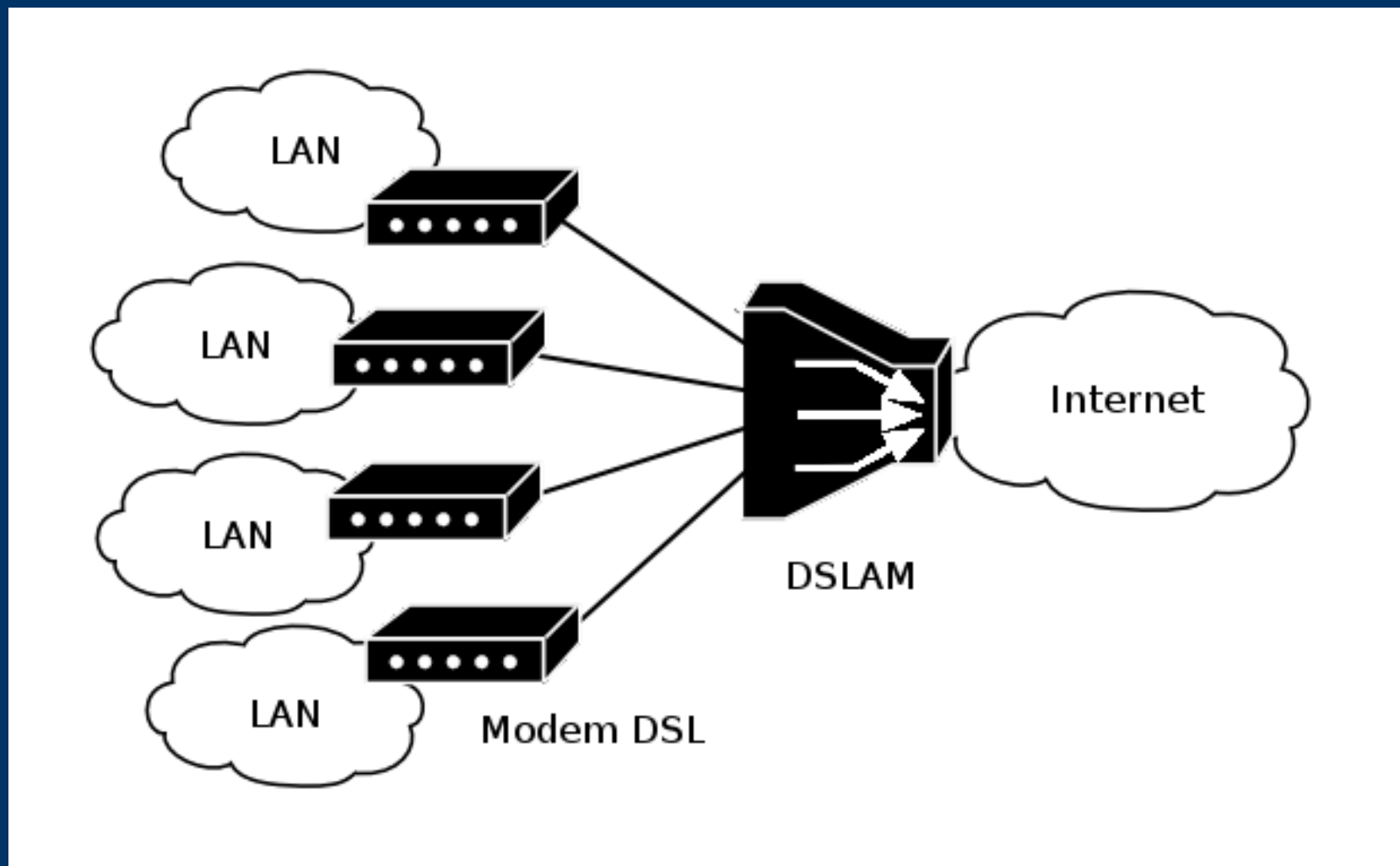


*Infrastruktura DSL Telekomunikacji Polskiej
z punktu widzenia bezpieczeństwa.*

Plan prezentacji

- xDSL, modemy
- Geneza problemu
- Odkrywanie słabości + demonstracja
- Co można było zrobić?
- Co nadal można zrobić?
- Czy można się zabezpieczyć?

Architektura xDSL



Modemy SpeedStream



5660



5100



4100

Geneza

- Uszkodzenie modemu/routera (terminologia)
- Modem *Planet*
 - DSL
 - PPP
- BOK
- Login i hasło
 - PPP tak
 - telnet nie (kontrola)



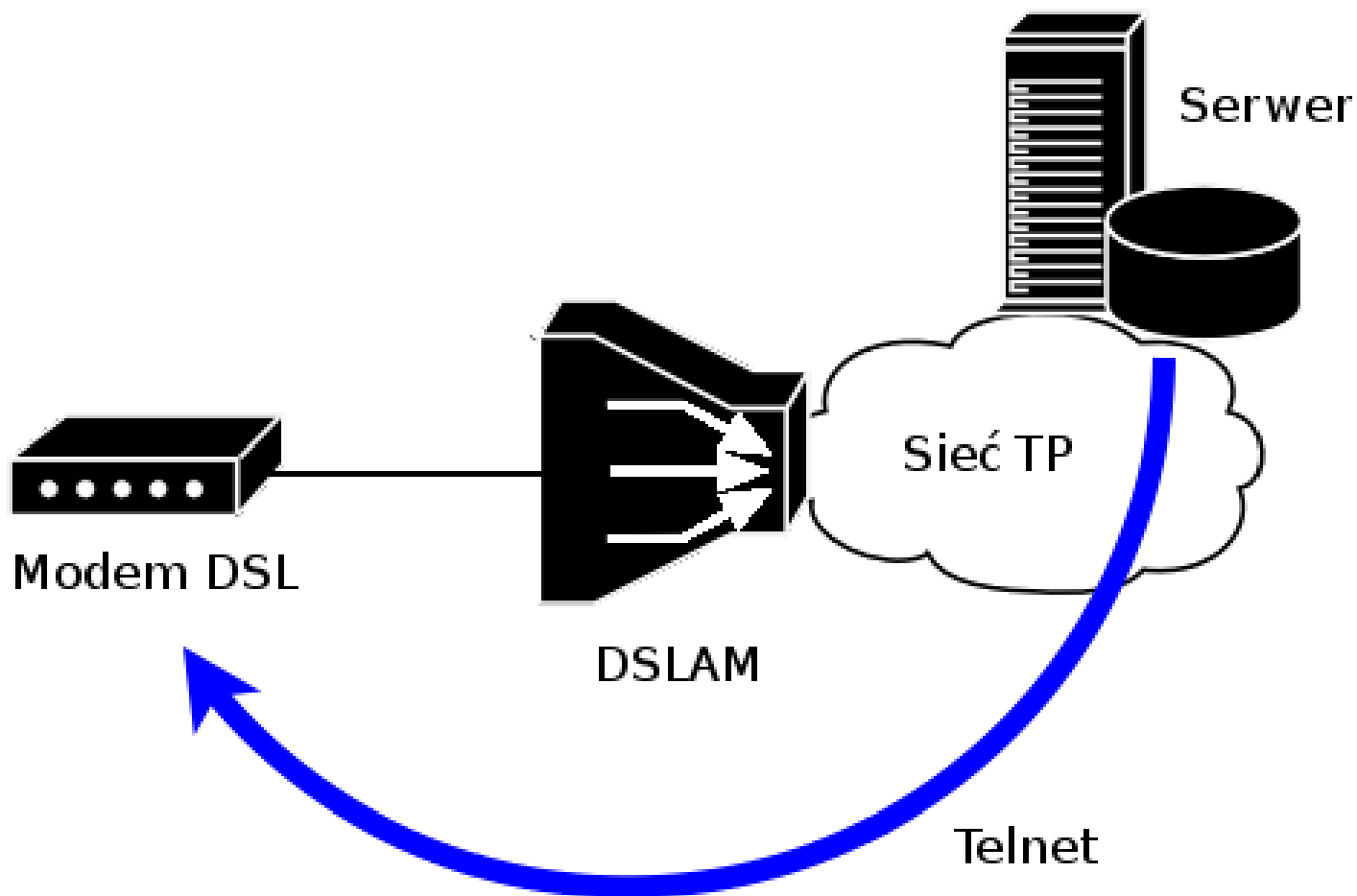
Kontrola nad modemem

- Oficjalne wytłumaczenie
- Bezpieczeństwo:
 - słabe/domyślne hasła
 - aktualizacja oprogramowania
 - izolacja od sieci DSL (modemy kablowe vs. Ethernet)
- Diagnostyka i naprawy:
 - abonent nic nie zepsuje
 - sprawdzanie parametrów (telnet, snmp)
- Organizacja:
 - obsługa użytkowników
 - dokumentacja dla użytkowników
- Usługi

Automatyczna konfiguracja

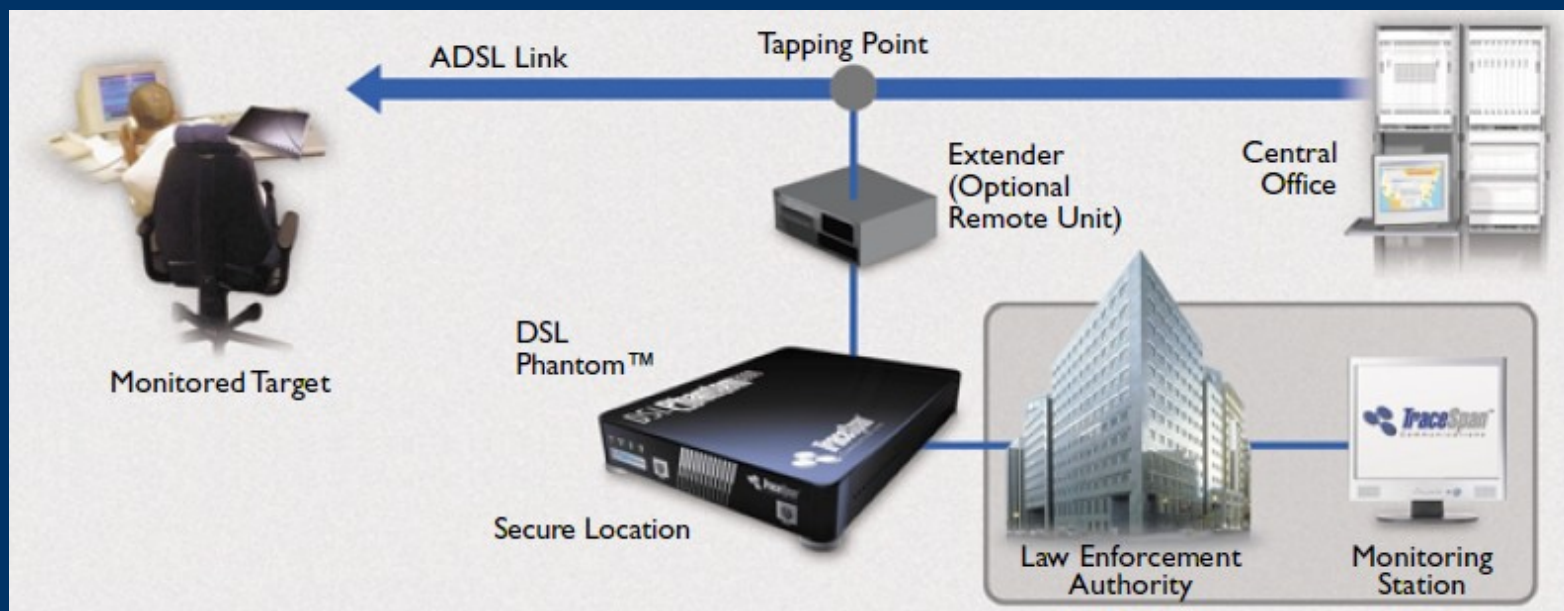
- Serwisowy login i hasło
- Ułatwienie przy instalacji
- Zabezpieczenie (nieuczciwy monter)
- *Pod SpeedStream*
 - instrukcja modemu 5660
 - skrypty?
 - zarządzanie
- Jak to działa?

Jak to działa?



Przechwytywanie transmisji

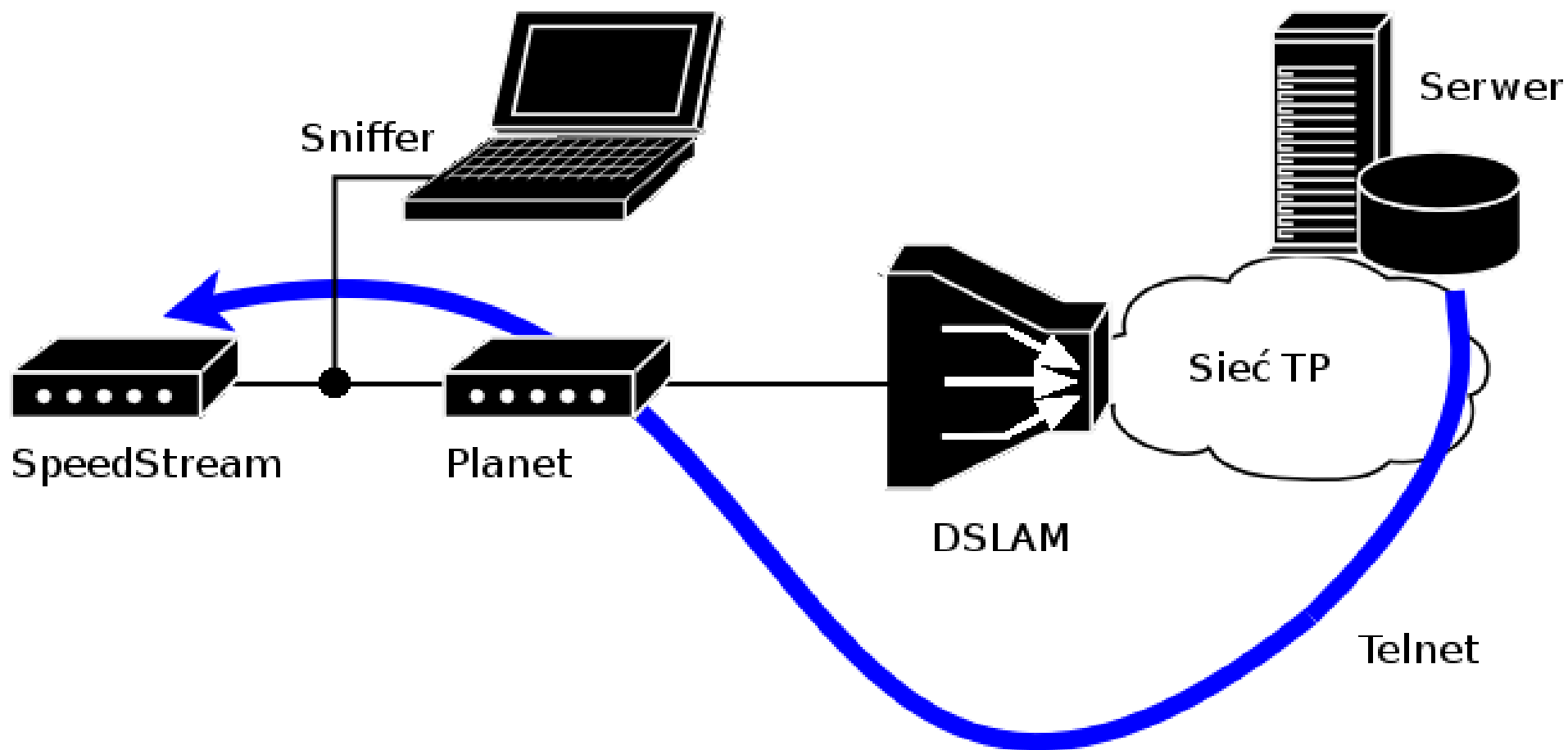
- DSL Phantom™
 - *passive ADSL tapping device, monitors and records data transparently within the ADSL physical layer*
 - http://www.tracespan.com/2_2LI%20Monitoring.html



Modem in the Middle (1)

- Modem *Planet*
 - login/hasło
 - NAT
 - przekierowanie portów
- Modem *Speedstream*
 - ustawienia fabryczne
 - trasa domyślna
- PC
 - Sniffer
- Akcja!

Modem in the Middle (2)



Analiza transmisji

1. show
2. set pppauth xxxxxxxxxxx@internetdsl
yyyyyyyyy
3. set napt disable
4. set ethip a.b.c.d 255.255.255.248
5. n
6. set snmpcfg zzzzzzzzz a a a
10.10.10.10 10.10.10.10
7. set password
8. zzzzzzzzz
9. zzzzzzzzz
10. reboot
11. y

- Nawiązanie połączenia
- Komenda *show*
- Zmiana parametrów
 - numer IP
 - hasła
- Reboot
 - zastosowanie zmian
 - zabezpieczenie
- Po co *show*?
 - MAC

Emulator modemu

- Perl
- Opcje telnetowe, znaki CR
- Konfigurowalny adres MAC
- Dowolny modem w Polsce!

Dostęp zdalny

- Telnet
 - działa lokalnie
 - połączenia na tcp/23
 - połączenia na inne porty
- Filtrowanie
- *tcptraceroute*

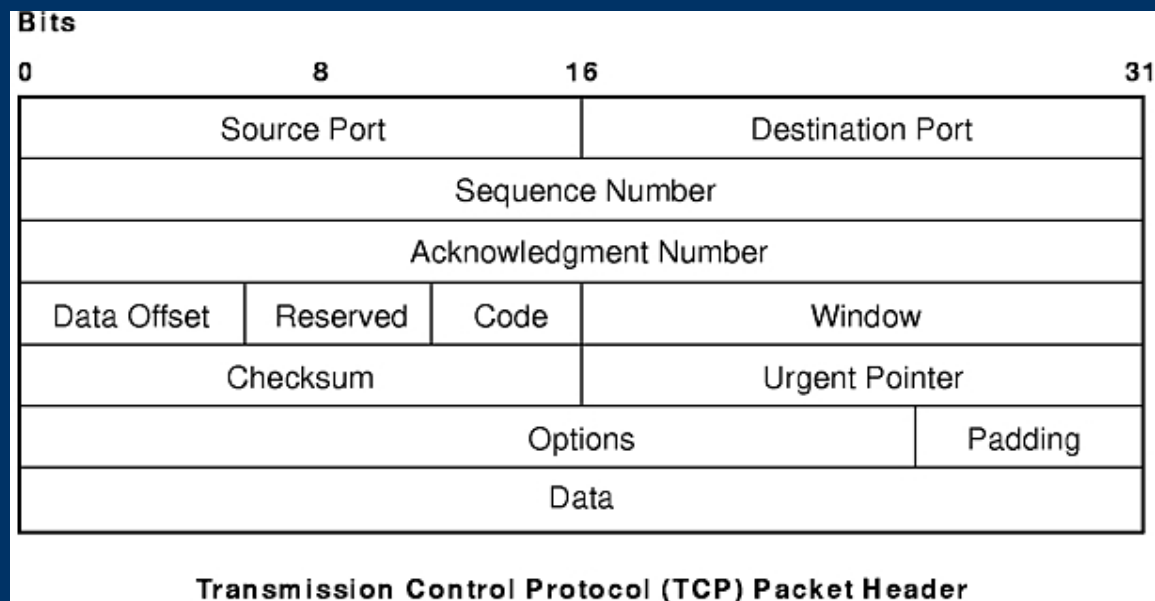
DSLAM

- Stinger™
 - Lucent Technologies to expand DSL management software for Telekomunikacja Polska's broadband network
 - Lucent has been supplying TP with broadband access solutions from its Stinger™ DSL family



Filtr pakietów

- Dodatek
- Wydajność
- Bezstanowy
- Fragmentacja
- *fragroute*
 - Flagi oddzielone od numeru portu
 - nagłówek (patch)
 - 8 bajtów
- *spoofing* (ISN)



Ataki

- Blokowanie łącza (chwilowe lub ciągłe)
- Zmiana hasła – TP traci kontrolę
- Włamanie do sieci wewnętrznej (NAT)
- Zniszczenie modemu (firmware)
- Komenda *set priv*:
 - zombie – DdoS, spam
 - Sniffer
 - MitM
- 35 tys. modemów (08.2004)
 - 8,7 Gbit/s

Jak zdobyć adresy MAC?

- Serwer
 - nie tylko adresy MAC
 - testowanie skryptu: *''; , zbyt dużo danych
 - *p0f*
 - firewall
- 6 bajtów
 - $2^{(6*8)} = 281.474.976.710.656$
 - $2^{(3*8)} = 16.777.216$
- Serie
- Limity czasowe
 - uzyskanie danych
 - przerwanie połączenia

SpeedStream 5100

- Dostęp przez www
 - częściowo otwarty
 - *fragroute*
 - status
- IP => MAC
- Skaner
- Inne CLI
 - skrypt przerywa działanie
 - *Planet* raz jeszcze
 - domyślne hasło admina



Aktualna sytuacja

- Przekazanie materiałów
- Filtrowanie ruchu do modemu
 - port 23
 - nie tylko SYN
 - www (MAC)
- Filtrowanie fragmentów z offsetem 8 – zawsze

Dane modemu

- Uzyskiwanie danych modemu – nadal możliwe!
 - 5660 (27.03-8.05) – *disclosure effect*?
 - 5100
 - przykładowe egzemplarze
 - ale co zrobić z danymi?
- Demonstracja

SpeedStream 4100

- Skrypt nie konfiguruje modemu
 - *show sys versions*
 - specjalne informacje?
 - zmiana procedury
 - reset + *Planet* + *sniffer*?
- Dlaczego tylko 4100?



Co można zrobić teraz?

- Modemy 5100
- Aktualność ACL
- Atak z wewnątrz
 - włamanie do sieci
 - administrator
 - MAC
 - Dostęp telnet (inny port + filtrowanie ip)
 - vxsniff
 - <http://www.xs4all.nl/~borkhuis/vxworks/vxsniff.c>
 - firmware
 - <http://www.tcniso.net/>
 - rootkit
- Przejęcie IP (pasmo, fałszywy serwer, *spoofing*)
- DSLAM (\$500, MitM = Phantom)

Zabezpieczenia?

- Czy mogę odczytać swoje hasło?
 - zmiana hasła
 - filtrowanie lub inny modem
 - port-forwarding, logowanie i *odbijanie z powrotem*
 - co na to TP?
- MAC:
 - router/firewall
 - zabezpieczenie fizyczne (naklejka z adresem MAC)
- Można też:
 - wnioskować do TP – wyłączenie autokonfiguracji
 - czekać (5660)

Dziękuję za uwagę.